INDUSTRIAL CONTROL SYSTEMS
Community of Interest

GUIDANCE: A MANUAL APPROACH TO ASSET MANAGEMENT IN INDUSTRIAL CONTROL SYSTEM / OPERATIONAL TECHNOLOGY ENVIRONMENTS.

Introduction

Complete asset registers are a fundamental part of managing cybersecurity risk. To understand the threat landscape within a facility, it is necessary to identify both non-network connected and connected assets and the vulnerabilities they may have. It is also important to understand the connections and dependencies between assets, as this will have an impact on maintenance and incident response planning.

In this article we shall be focussing specifically on a manual approach to asset visibility within Industrial Control System (ICS)/OT environments and how it can be a useful alongside other approaches to understanding assets.

NCSC has generalised asset management guidance which can be found here - https://www.ncsc.gov.uk/guidance/asset-management, while this article is part of a series of Operational Technology (OT) specific guidance articles on Asset Management first introduced here and hosted on the ICS Community Of Interest (ICS COI) website. NIST in the US have also published related guidance that can be found here.

Asset discovery and maintenance of asset registers within an ICS/OT environment can be very difficult. ICS/OT systems are often designed to last a minimum of 25 years, and many systems are in service much longer than that. Over time, parts are replaced, systems are modified for new requirements and new systems are added. If accurate records of these changes are not maintained, then it is easy to lose track of what is installed. In addition, the data required about each asset will naturally change over time, maturing with the ICS/OT security discipline of the Asset Owner. ICS/OT network security was not a mature discipline when older systems were designed, so information about network configurations, MAC addresses, firmware versions etc. would not have been recorded in a centralised location.

When designing a new industrial control system, or making major (security) upgrades, it is important to design for asset management. Meaning, design systems that are capable of automatic asset management; design systems that are easy to maintain.

However, with existing ICS/OT systems, asset owners do not have that luxury. Segregation makes it difficult to deploy sensors to identify all assets continuously, legacy components may react badly to active scanning techniques and original documentation may have been long lost or is no longer accurate.

Meet Admin Corp

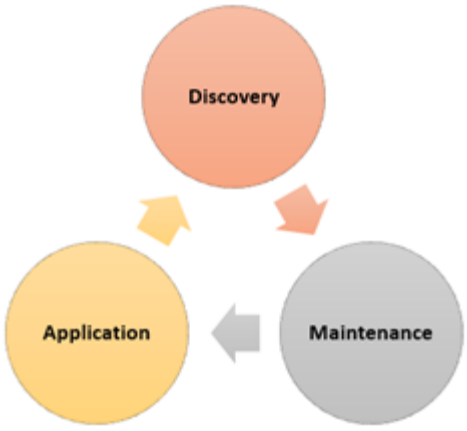
Admin Corp is a fictional organisation that produces Adminox, a highly volatile, refined form of administrative paperwork that is essential to every organisation in the country. It is created from volatile raw products using a continuous chemical process.

As an essential service, Admin Corp must comply with the EU NIS Directive. This means that Admin Corp's network, information systems and technology needed for the production of Adminox must be protected from cyber-attack.

Admin Corp are regulated for safety by the UK Health and Safety Executive. Therefore, they must take steps to ensure the continued safety of the Adminox production process.

Adminox processing plant

As the first Admin Corp factory has aged and original documentation was lost through a series of acquisitions; they have lost track of their assets. Their networks are highly segregated preventing the use of centralised scanning tools, and there are concerns that active scanning could cause a disruption in the process - potentially a threat to safety. So how can Admin Corp regain control of its assets?



Three phases of Asset Management

There are 3 phases to successfully managing assets:

- **Discovery:** is ensuring that new systems are added to the asset register "as commissioned" and adding existing undocumented systems to the register.
- **Maintenance:** is ensuring that all modifications to systems are recorded, and that records on existing assets are complete.
- **Application:** is using the asset register to manage risk.

The following sections define how Admin Corp manages its manual asset management system.

Manually maintaining asset inventories in a spreadsheet, or database, is not best practice, although commonly used. When they are used it is important that proper change control procedures are utilised (including versioning of the document, and dated details of changed in the assets themselves). While actively using these techniques will help to maintain the asset register, they take time and are reliant on active and sustained participation by all stakeholders. In a busy industrial environment, it will remain difficult to keep on top of maintaining the asset register, unless properly embedded within the change management process. ***Asset owners should strongly consider the use of an ICS/OT specific automated asset discovery tool or process to support the maintenance of the asset registers.***

Asset owners should also consider a hybrid approach. While an automated asset discovery tool may not be able to capture the entire ICS/OT network, if it can capture part of it using automated means, then that is better than managing the asset registers entirely manually. Unfortunately, at this stage of their ICS/OT Cyber security journey, Admin Corp have neither invested in automated asset discovery tools (although they are exploring options) or an ICS/OT specific asset management database (having an extensive IT CMDB system in place), and therefore as an interim approach for their ICS/OT environment, are utilising an approach based around use of Microsoft Excel spreadsheets.

It is important to note that any Asset database/register and the information collated via this approach would be of high value to a Threat Actor and steps should be taken to ensure it is suitably protected at rest and when in transit.

Discovery

New Systems

When purchasing a new system, or designing a new system internally, the system supplier should be required to provide the information for the network asset register as a project deliverable. This also applies when designing a significant modification to a system. The Admin Corp purchaser/project manager therefore imposes the following requirements on the supplier:

- The system asset register must be "**as commissioned**".

During the design of the new system, the project asset register will be constantly changing and evolving, so only the final version will be required for inclusion into an existing asset database.

Nevertheless, Admin Corp makes the supplier aware of the information required early in the project, as some additional effort is required to gather the information.

- The system asset register must be **verified as complete by inspection as part of acceptance testing**.

Due to the volatility of the project asset register during design, the supplier should verify its accuracy during acceptance testing of the system, to check that it has been updated as the design has changed. This could be a manual verification (or could utilise passive or active scanning techniques). The Admin Corp Project Managers therefore enforce that verifying the asset register is one of the first checks during factory & site acceptance testing procedures.

- The system asset register must be submitted in **editable format**.

If the document is provided in a non-editable format, such as PDF, then inputting the data into an existing asset register will be very difficult, therefore Admin Corp ensure that the document is supplied in its original, editable format.

- The system asset register must include all fields required by any **existing asset management system**.

The Admin Corp asset owner provides a template format to the supplier, in order to ensure that the asset register is submitted in a format that is easily importable into the existing asset register, and that included all the fields required.

Enforcing this system on new and significant changes to systems will ensure that the data in the asset register is complete, as it was commissioned. However, systems are not static and evolve over time. The next challenge is maintaining the data.

Existing Systems

Admin Corp also needs to identify its existing assets. To do this it has engaged a security service provider to identify their existing assets. This is a process called Asset Discovery.

Asset discovery of existing systems can comprise of the following steps:

- Document Review
- Interviews & Walkabouts
- Passive Scanning
- Active Scanning

Admin Corp worked with the security service provider to prioritise and order the above methods to suit its environment and capability.

Document Review - Control systems will usually have been supplied with a technical file that includes documents such as a functional design specification, hardware bill of materials, software bill of materials, IP address register, network diagrams and electrical schematics. These documents should provide all the information required to form a basis for the asset register, however, in Admin Corp's case, these documents have not been maintained over the years as the control system has changed and evolved.

Interviews and Walkabouts - Admin Corp has assigned each system to a responsible engineer that has specialised in maintaining their system. While the existing documentation may be incomplete, the responsible engineer that maintains it may be able to fill in additional details that are missing from the documentation. Interviews are arranged with these engineers to ensure that any additional information they can add is captured.

Sometimes, the only way to find out what is there is by walking around the ICS/OT environment and looking. If, during interview, the responsible engineer identifies a system/asset but does not know sufficient technical detail about it then physically looking at the control panel can help fill those gaps. Most ICS/OT assets have the part number printed on them somewhere, which can be researched later. It also helps to check that there are the expected number of network cables leaving the panel. Too many or too little is an indication that a connection has been forgotten about. Admin Corp gains great benefit from these walkabouts, documenting each site/asset in a similar manner, while ensuring that everything in each bay or production area is accounted for.

Passive Scanning - Passive scanning is where a tool (such as a piece of software, virtual machine, or hardware appliance) is used to analyse network traffic. For example, a laptop running a packet capturing tool can be connected to the network, so that it can record network traffic. By analysing the resultant network recording (PCAP) file, it is possible to identify information about the assets, and their connections.

However, this does have vendor related limitations in terms of how much data can be identified from the network recording. It only identifies information assets that were active while the tool was running. This method catches a snapshot of what was communicating during the period it was plugged in. So, if a pair of devices only communicate once a day, and the tool was only analysing

network traffic for a couple of hours, then that connection would be missed. It also only captures what assets were communicating across the switch that the tool is connected to, so it may be necessary to run the probe in multiple places to get better coverage. Assets that are only communicating locally without passing through the core switches, may be missed entirely.

A potential part solution would be to passive analysis undertaken on network recordings captured over a prolonged period (e.g., 2-4 weeks), avoiding maintenance windows. That would maximise opportunity to see assets which speak infrequently on the network, but also enable captured of assets introduced periodically on the network during that time which might otherwise be missed.

There are few techniques, referred to as **intelligent interrogation** that will be covered in later guidance articles, that can be used to enrich the network traffic with relevant data the tool is specifically looking for:

- Invoke engineering related traffic to the assets – e.g., Rockwell RSLinx or Siemens TIA portal can be leveraged to enumerate relevant asset data.
- Wide-scale analysis in an attempt to catch broadcast traffic. Vendor related specifics allow some components such as PLCs, RTUs to broadcast asset information on the network every few minutes or so. If Admin Corp have assets that contain this behaviour (and even if Admin Corp have unmanaged switches) connecting to a switch with the tool for a few minutes may be worthwhile.

In both cases these techniques trigger assets to send asset information related information over the network that the passive scanning tools can analyse and process into an asset register. A third technique is also available, but highly dependent on the assets (vendor) of Admin Corp's ICS:

- Analysis based on configuration files. Some passive scanning tools have a feature that allows Asset owner to import PLC or RTU configuration files that contain relevant asset information and use this to enrich its database (in addition to the network traffic analysis). If Admin Corp engineers store their PLC configuration files in a centralized place, a quick win would be to import these into the tooling for asset register creation. A manual process can also be established to find relevant information in these files, but tooling can process large batches of configuration files within few seconds.

While Admin Corp would have liked to conduct passive scanning of the network, unfortunately due to the limited opportunity for access to IP enabled switches, and the plethora of ICS related protocols, serial links etc within their ICS/OT environment of their original factory, this was not possible. They were, however, manually able to utilise configuration information extracted from network appliances such as switches and routers to gain information about hardware addresses of devices on the network and IP numbers allocated, to help gain understanding of the way assets were addressed on the network.

Active scanning - Active scanning can also be utilised to fill out the asset register, but consideration should always be given to the potential impact these techniques will have on process safety. Active scanning works by sending requests to network assets to gather information. It does this by simulating engineering workstations and corresponding traffic much like the techniques that were discussed earlier to enrich the asset register during passive scanning.

The difference between passive and active scanning here, is that passive scanning uses techniques that are non-intrusive to the environment by leveraging fully supported and qualified vendor tooling that are known to be safe. Active scanning mostly relies on simulating this behaviour and could potentially trigger requests that some ICS/OT equipment is unable to handle. This may cause ICS/OT assets to behave unexpectedly, which could compromise safety, or functionality of the control system.

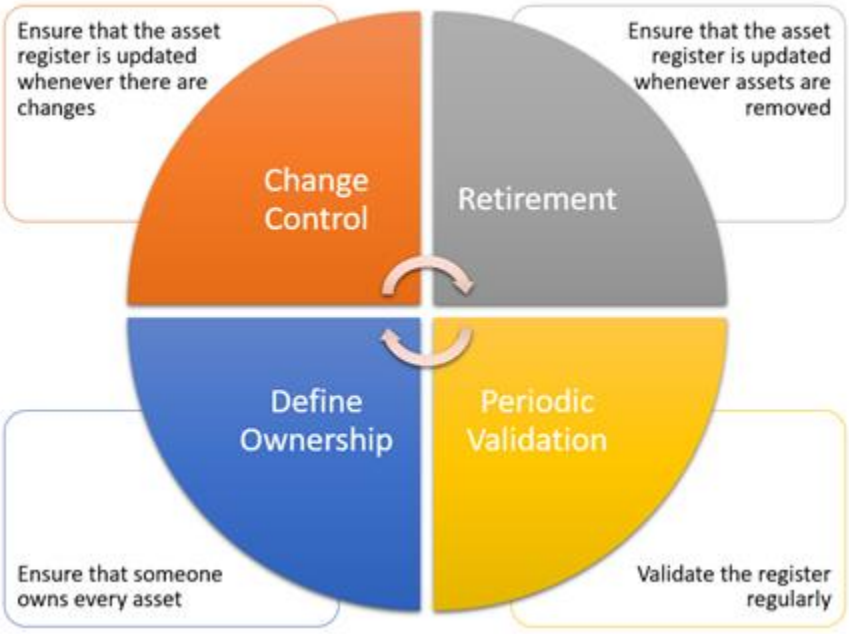
Looking at different active scanning tools, their levels of protocol and vendor support vary. Some suppliers of such active scanning tools have partnerships with major OEMs/Vendors (Siemens, Rockwell, etc.) and that may provide some assurance that the active scanning tools are qualified or known to be safe for use for certain device types and or protocols. (These are covered under the **Active Scanning/Intelligent Interrogation** guidance to be issued shortly).

Active scanning should only be attempted by a suitably qualified and experienced person, who understands the potential risks. Active scans should be limited in scope to target specific IP addresses, rather than targeting entire subnets.

Admin Corp considered the merits and risks of conducting Active scanning on their operational networks and decided that the risk to un-intended consequences, such as loss of productivity was too great for them to undertake this approach, hence them concentrating on a purely manual approach to asset discovery.

Maintenance

In the discovery phase, Admin Corp manually captured a snapshot of how the network assets look now, but they also need to ensure that the asset register is maintained over time. This will involve changes to the organisation's change control procedures and periodically validating the asset register.



Change Control

Whenever a modification to a system is made, the responsible engineer should ensure that the asset register is update., this should include the changes made to the asset and the person(s) responsible for the change, showing history of both. This is also an opportunity to check that the asset register details are currently correct for the whole system being modified.

Admin Corp added this process to their change management procedure, to ensure that it is completed for every change. The change management procedure is regularly audited, albeit manually, to ensure that the asset registers are being updated as required.

Retirement

Admin Corp also include updating the asset registers in its decommissioning and secure asset disposal procedures. This procedure again is regularly audited to ensure that the asset registers are being updated as required.

Periodic Validation

Admin Corp, also request the responsible engineers validate the asset register periodically (within Admin Corp this is done every six-months) to confirm that it is still accurate, as they understand, for the systems that they are responsible.

This activity could be supported with periodic validation using passive and active scanning techniques. It could also be externally validated by security solutions provider, although Admin Corp due to budget challenges rely on the responsible engineers doing the validation.

Define Ownership

Admin Corp has assigned each system to a responsible engineer, however, the asset management system needs to ensure that someone is responsible for every asset. Sometimes, shared infrastructure is forgotten about, as every system asset owner thinks that it falls under someone else's responsibility. Admin Corp therefore ensure that every asset is owned by someone, their scope is clearly defined, and they know what their responsibilities are.

Application

Admin Corp is confident that their asset register is an accurate representation of their ICS/OT estate, and is regularly updated, albeit manually. They therefore use the asset register to support the following activities:

- **Risk management:** understanding and managing cyber risk depends on ICS/OT assets being accounted for. If assets are allowed to slip under the radar, it will not be apparent if appropriate security controls are missing, resulting in unmanaged risks.
- **Managing legacy:** in ICS/OT systems assets often have a much longer lifespan than in IT systems. Admin Corp update the asset registry when asset fall out of vendor support for instance. Using the asset register to identify assets that are no longer supported by the vendor, allows Admin Corp to assess the risk of not replacing them and create contingency plans for when they fail.
- **Identity and access management:** being able to identify users and devices is necessary in order to implement an effective identity and access management system. The asset register helps ensure all users and devices have unique identities and identifies assets and resources that need access controls applied.
- **Vulnerability and patch management:** patch management in ICS/OT systems can be controversial. It may be necessary to wait for a planned shutdown to apply patches, in some cases, applying patches will require testing or re-validating system functionality (which can be very expensive) and patches may no longer be available for legacy asset that can't be replaced. Admin Corp use the asset register to identify which vulnerabilities present a realistic risk, then decide whether to transfer, tolerate, treat (with appropriate mitigations/controls) or terminate the risk. Admin Corp also use the asset register to record that decision so that when the situation changes, it can be revisited. The asset register is also used to help plan the list of things to do with regards patch management in the next planned shutdown.
- **Incident management, response and recovery:** Given Admin Corp, using the asset register provides them with in-depth knowledge and understanding of their assets, allows them to determine which are most critical to the organisation (Via the likes of Crown Jewels Analysis) helps them plan for, respond to, and recover from incidents. By ensuring nothing important is missed and having the right information available, they are able to act quickly and minimise disruption. Configuration information can also provide a benefit to incident response/recovery planning, by utilising this as an opportunity to hash known good firmware/configurations for devices and take back-ups to support recovery efforts.
- **It's not just cyber security**: most business operations depend on some aspect of asset management. This includes IT operations, financial accounting, managing software licences, procurement, and logistics. While they may not all need the same information, there will be some overlap and dependencies between the respective requirements. The security aspect should not be considered in isolation or as the primary consumer of asset information, so integrating and coordinating asset management across your organisation will help reduce or manage any conflicts between these functions.

Final Thoughts

Admin Corp realise that their manual asset management system is not ideal but recognise that even a manual asset management system can bring significant benefits both to security and ongoing maintenance efforts. Admin Corp note that they will struggle to keep the register up to date, and vulnerability management will be difficult without automated tools/processes to identify and match asset information against latest available vulnerability information.

Admin Corp therefore in the future will be looking to explore a hybrid approach, where an automated asset management tool is combined with manual methods, noting that this will significantly reduce the burden on ICS/OT engineering team to keep the asset register up to date. Some automated asset management tools have the capability to import asset lists obtained by other means, so all assets can be managed in one place.

The asset database/register can now be considered a single source of truth, which will benefit the IT teams, the ICS/OT engineering and maintenance teams and the business overall.

Admin Corp also realise that their Asset database/register and the information collated via this approach would be of high value to a Threat Actor and have taken steps to ensure it is suitably protected at rest and when in transit.

CAF IGP Summary

This case study discusses measures that contribute to the following CAF IGPs (V3.1):

- **A3.a A01**: All assets relevant to the secure operation of essential functions are identified and inventoried (at a suitable level of detail). The inventory is kept up to date.
- **A3.a A02**: Dependencies on supporting infrastructure (e.g. power, cooling etc) are recognised and recorded.
- **A3.a A03**: You have prioritised your assets according to their importance to the operation of the essential function.
- **A3.a A04**: You have assigned responsibility for managing physical assets.
- **A3.a A05**: Assets relevant to essential functions are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.
- **B4.b A01**: You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of the essential service.
- **B4.b A02**: All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment.
- **B4.b A04**: You regularly review and validate that your network and information systems have the expected, secured settings and configuration.
- **B4.d A01**: You maintain a current understanding of the exposure of your essential service to publicly known vulnerabilities.
- **C1.c A03**: Alerts can be easily resolved to network assets using knowledge of networks and systems.
- **C1.e A07**: Monitoring staff are aware of essential services and related assets and can identify and prioritise alerts or investigations that relate to them.

Statement of Support

This guidance has been produced with support from the Thales Cyber Consultancy and members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected Cyber-Physical Systems (RITICS), with support from the National Cyber Security Centre (NCSC). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.

This document is provided on an information basis only, the Thales Cyber Consultancy, ICS-COI members and NCSC have used all reasonable care in verifying the guidance contained within using the data sources available to it, they provide no warranty as to its accuracy or completeness. To the fullest extent permitted by law, The Thales Cyber Consultancy, the NCSC, and the ICS-COI accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using this document. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favour by the Thales Cyber Consultancy, the ICS-COI or NCSC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.